ABSTRACT

A method and system for evidencing payment of indicia using secret key cryptography is disclosed. The method and system include a plurality of indicia generating devices that are divided into groups for generating and printing indicia on a media that is to be received at a plurality of establishments, wherein the establishments are associated with different geographic designations. The method and system include assigning a plurality of verification keys to each indicia generating device in each of the groups, wherein each of the verification keys assigned to each of the groups is encrypted as a function of a respective geographic designation. A key ID is associated with each of the verification keys and is encrypted as a function of the same geographic designation used to encrypt the corresponding verification key. After the verification keys and key ID's are assigned, each one of the establishments receives the verification keys and the key ID's that were encrypted as a function of the geographic designation associated with the establishment. When generating indicia for media destined for a particular one of the establishments, the indicia generating devices evidence the indicia by generating one of the verification keys and the corresponding key ID assigned to indicia generating device's group based on the geographic designation associated with the particular establishment, and uses the generated verification key to create a digital signature. The indicia generating devices digitally sign the indicia by including the digital signature and the generated key ID in the indicia. Upon receiving the media at the particular establishment, the indicia on the media is verified by using the key ID on the indicia and the distributed verifications keys to compute a digital signature, and comparing the computed digital signature with the digital signature on the indicia.